

CYBERCRIME SURVIVAL GUIDE



WOLF



PACK

CONTENTS

02.

INTRODUCTION

06.

CYBERBULLYING

10.

CST - DON'T FALL VICTIM TO CYBERBULLYING

12.

PHISHING

14.

CST - USE YOUR PHISHING COMMON SENSE

16.

CST - INSPECT LINKS BEFORE CLICKING

18.

CST - DON'T OPEN EMAILS OR ATTACHMENTS FROM UNTRUSTED SOURCES

20.

RANSOMWARE

22.

CST - KEEP YOUR SOFTWARE UP TO DATE

24.

CST - INSTALL ANTIVIRUS ON ALL DEVICES

26.

CST - REVIEW APP PERMISSIONS BEFORE INSTALLING AN APPLICATION

28.

CST - PROTECT YOUR DATA

30.

TOP ONLINE SCAMS

34.

CST - CREATE STRONG AND UNIQUE PASSWORDS

36.

CST - LOG OFF

37.

CST - BE CAUTIOUS WHEN USING BLUETOOTH AND WI-FI

38.

WHERE TO APPLY THE CYBERCRIME SURVIVAL TIPS

39.

STAYING SAFE ON SOCIAL MEDIA

42.

GLOSSARY

44.

SOURCES

Disclaimer

Wolfpack Information Risk (Pty) Ltd does not guarantee or offer assurance that this document will completely protect or keep you 100% safe from cybercrime. The information and applications mentioned in this document may contain errors and are subject to change. Wolfpack Information Risk (Pty) Ltd is not responsible for any loss, damage, or disruption that may be caused by errors, omissions or the use of the applications / software mentioned, whether such errors or omissions result from negligence, accident, or any other cause. Moreover, Wolfpack Information Risk (Pty) Ltd is not responsible for the functioning of any of the links to related websites (including ease of downloading programs, or purchase support and fulfillment). The Cybercrime Survival Guide publication is owned by Wolfpack Information Risk (Pty) Ltd. No part of this publication may be reproduced or transmitted in any form without explicit prior permission from Wolfpack Information Risk (Pty) Ltd. The opinions expressed in the Cybercrime Survival Guide are not those of the publishers, who accept no liability whatsoever arising in connection with the contents of the publication.

All rights reserved.

© 2018 Wolfpack Information Risk (Pty) Ltd
www.wolfpackrisk.com



INTRODUCTION

Cybercrime is a very real threat. Victims today are losing substantial amounts of money and data. In many instances their privacy and even personal safety may be compromised.

The perpetrators realise the rewards are high and the risks are low. Modern cyber criminals are relentless opportunists - patient, strategic, bold and well organised - operating below the radar for as long as possible.

With the rapid evolution of cyber threats, it is understandable that the average person may feel paralysed by the sheer volume of dangers out there. Where can the average person obtain reliable guidance and the tools to protect their families, assets and information?

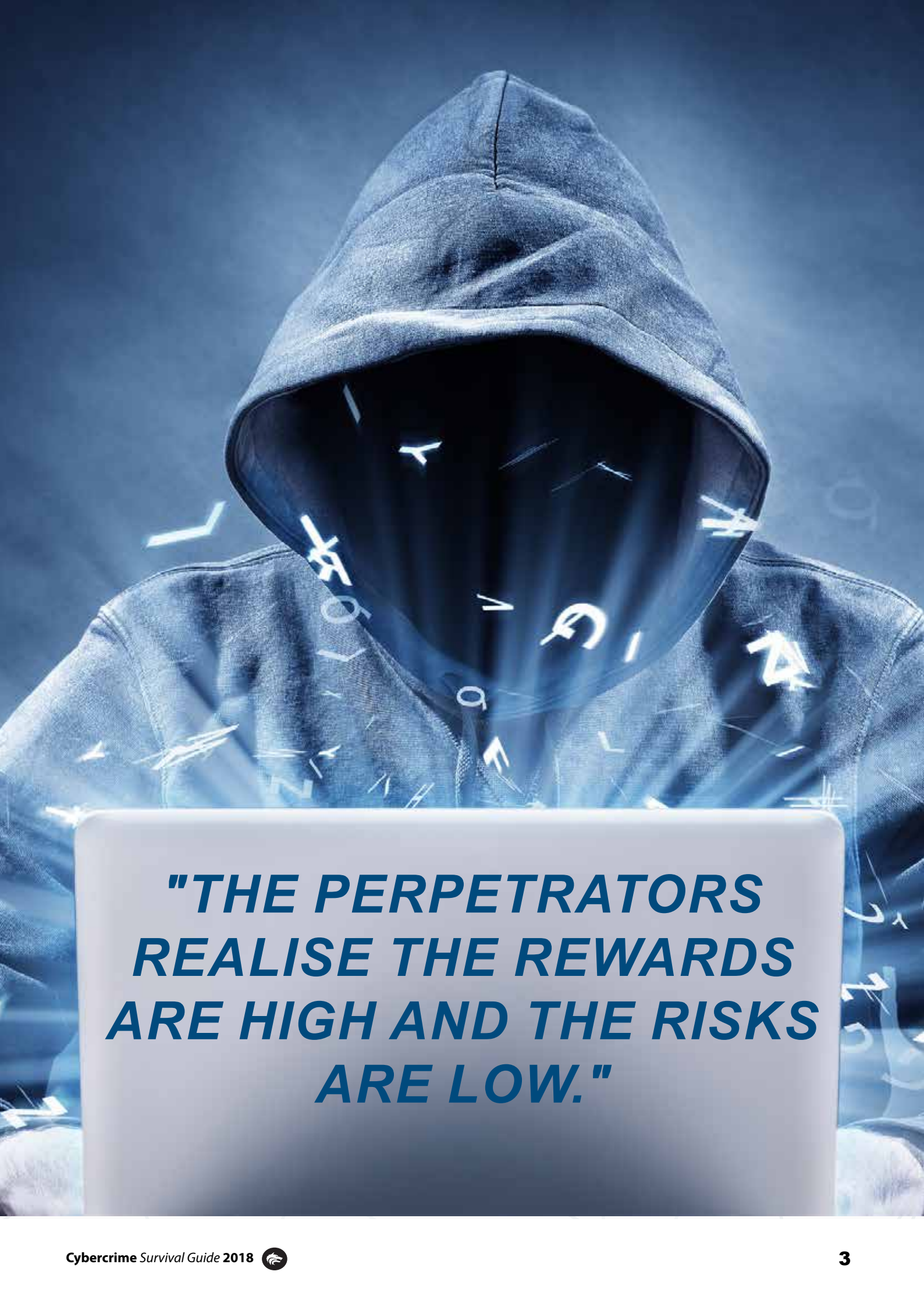
Cyber criminals are not just after money your personal information may be just as valuable.

The goal of the Cybercrime Survival

Guide is to raise awareness of the potential cyber risks you may face and to provide you with a non-technical approach to PROTECT yourself online.

The guidance offers valuable tips for cloud users, personal computers and mobile devices to ensure that your own private and financially sensitive information is kept safe.

You don't have to be a computer guru to use this guide.



***"THE PERPETRATORS
REALISE THE REWARDS
ARE HIGH AND THE RISKS
ARE LOW."***

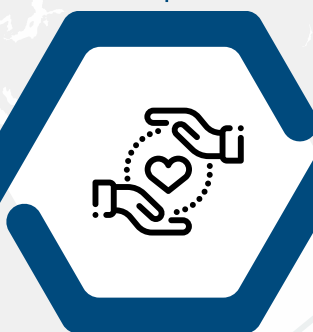
Each Cyber Survival Tip (CST) contains the following sections:

Quick Tips

This section provides you with a number of things you can do quickly in order to achieve the goals of the CST.

Why Should I Care?

This section highlights why the specific CST is necessary and what the consequences could be of not using the CST.



Getting Hands On

This section provides more detailed guidance on how to better protect yourself and your devices.

Helpful Websites/ Applications

This section contains a list of websites and applications which can assist you to meet the objectives of the specific CST.

Icon keys

are used to indicate where each CST can be used



Personal Computer



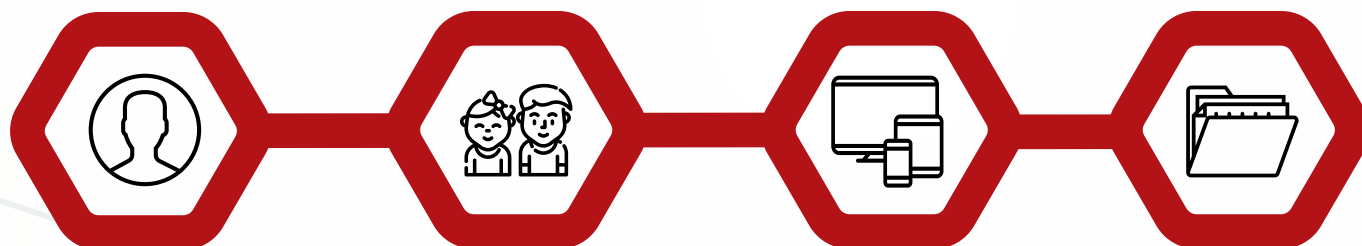
Internet



Mobile Devices

Impacts

Impacts are separated into four categories: Personal, Children, Devices and Data.



Personal

Children

Devices

Data





Definition:

Willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.

Referring to incidents where adolescents use technology to harass, threaten, humiliate, or otherwise hassle their peers. For example, youth can send hurtful texts to others or spread rumors using smartphones or tablets. Teens have also created web pages, videos, and profiles on social media platforms making fun of others. With mobile devices, adolescents have taken pictures in a bedroom, a bathroom, or another location where privacy is expected, and posted or distributed them online. Others have recorded unauthorized videos of their peers and uploaded them for the world to see, rate, tag, and discuss. Others are using embracing anonymous apps or the interactive capabilities on gaming networks to tear down or humiliate others.

What are some negative effects that cyberbullying can have on a person?

There are many detrimental outcomes associated with cyberbullying that reach into the real world. First, many targets report feeling depressed, sad, angry, and frustrated. Those who are victimized by cyberbullying also reveal that they are often afraid or embarrassed to go to school. In addition, research has revealed a link between cyberbullying and low self-esteem, family problems, academic difficulties, school violence, and various delinquent behaviors. Finally, cyberbullied youth also report having suicidal thoughts, and there have been a number of examples in the around the globe where youth who were victimized ended up taking their own lives.

Where does cyberbullying commonly occur?

Cyberbullying occurs across a variety of venues and mediums in cyberspace, and it shouldn't come as a surprise that it occurs most often where adolescents congregate. In the early 2000s, many kids hung out in chat rooms, and as a result that is where most harassment took place. In recent years, most youth are have been drawn to social media such as Instagram, Snapchat, Musical.ly, Twitter and video sharing sites such as YouTube. This trend has led to increased reports of cyberbullying occurring in those environments. We are also seeing it happen with portable gaming devices,

in augmented reality (AR) and virtual reality (VR) environments. In social gaming sites and in anonymous apps that come and go on a regular basis.

Cyberbullying vs. traditional bullying

While often similar in terms of form and technique, cyberbullying and bullying have many differences that can make the latter even more devastating. With the former, victims may not know who is targeting them or why. The aggressor can cloak his or her identity using anonymous email addresses or pseudonymous screen names. Secondly, the hurtful actions of those who cyberbully can go viral; that is a large number of people at school, in the neighborhood, in the city and the world can participate in the victimization or at least find out about the incident with a few keystrokes or touchscreen impressions.

The pool of potential targets, aggressors, and witnesses/bystanders is limitless. Thirdly, it is often easier to be cruel using technology because cyberbullying can be done from a physically distant location and the aggressor doesn't have to see the immediate response by the target. In fact, some teens simply might not realize the serious harm they are causing because they are sheltered from the victim's response. Finally, while parents and teachers are doing a better job supervising youth at school and at home, many adults don't have the technological understanding or time to keep track of what teens are up to online. As a result, a target's experience may be missed and an aggressor's actions may be left unchecked. Even if those who bully are identified, many adults find themselves unprepared to adequately respond.

Why is cyberbullying becoming a major issue?

Cyberbullying is a growing problem because increasing numbers of kids are using and have completely



embraced online interactivity. A remarkable 95% of teens are online, and the vast majority access the internet on their mobile device.

They do so for school work, to keep in touch with their friends, to play games, to learn about celebrities, to share their creations or for many other reasons. Online communication tools have become such a tremendous part of their lives, it is not surprising that some youth have decided to use the technology to be malicious or menacing toward others. The fact that teens are constantly connected to technology means they are susceptible to victimization and able to act on mean impulses toward others around the clock. Some adults have been slow to respond to cyberbullying, many feel that there are little to no consequences for their actions. Many even feel that there is little chance of detection and identification, let alone sanction. Cyberbullying crosses all geographical boundaries. Online connectivity across a broad variety of devices has opened up the whole world to users, and for the most part this has been a good thing. Nevertheless, some kids feel free to post or send whatever they want while online without considering how that content can cause harm.

The role of parents

The best path parents can take when their child is cyberbullied is to make sure they feel and are safe, and to convey unconditional support.

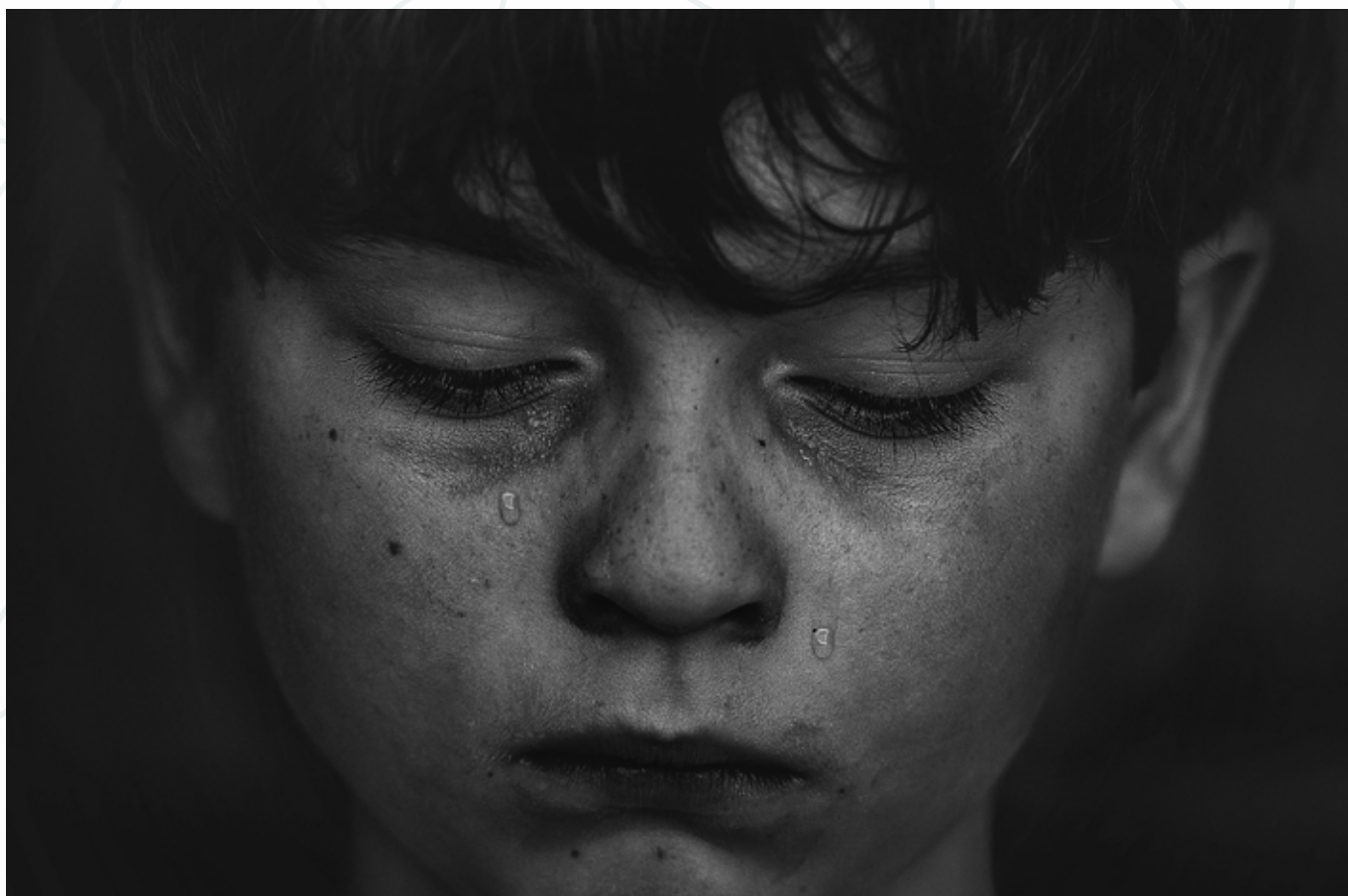
Parents must demonstrate to their children through words and actions that they both desire the same end result that when cyberbullying occurs life does not become more difficult. This can be accomplished by working together to arrive at a mutually agreed upon course of action, as many times it is appropriate and important to solicit the child's perspective as to what might be done to improve the situation. It is so critical not to be dismissive of their perspective, but to validate their voice and perspective. Targets of cyberbullying and those who observe it must know for sure that the adults who they tell will intervene rationally and logically, and not make the situation worse. If it is deemed necessary, parents should explain the importance of scheduling a meeting with school administrators or a teacher they trust to discuss the matter. Parents may also be able to contact the father or mother of the offender, or work with the internet service provider, cell phone service provider, and content provider to investigate the issue or remove the offending material as many times as the victim wants including the content or account deleted so they can move on with their life. The police should also be approached when physical threats are involved or a crime has possibly been committed extortion, stalking, blackmail, sexual exploitation of minors, etc.

Overall, parents must educate their kids about appropriate online behaviors just as they convey appropriate offline behaviors. They should also monitor their child's activities while online. Especially early in their exploration of cyberspace. This can be done

informally through active participation in your child's internet experience, which is recommended most of all and formally through software. Spying on kids and unnecessarily invading their privacy should only be done as a last resort when there is a significant cause for concern. Honest and open monitoring is a part of a healthy parent-child relationship. Spying conveys distrust and may encourage youth to go further underground.

In time parents will need to give their children more freedom, privacy, and responsibility. They will not be able to monitor their child's activities 24/7, nor should they need to do so. As a result, it is crucial that parents cultivate and maintain an open, candid line of communication with their children, so that they are inclined to reach out when they experience something unpleasant or distressing online. Reinforce positive morals and values about how others should be treated with respect and dignity. Point out models to emulate in society and use viral mistakes made by other youth and adults as teachable moments. Resilience is the skill to bounce back after facing adversity. It is also important to cultivate with intention at this stage. Instead of swooping in and rescuing kids from all of their social and relational struggles, help them hone the ability to deflect, disrupt, dispute, shrug off, or otherwise ignore hurtful things that others say or post. This can occur by helping them internalize positive beliefs rather than self-defeating thoughts after being cyberbullied, or by spotlighting relatable overcomers in books and movies with whom they can connect. Parents may

also utilize an age appropriate "Technology Use Contract" to foster a crystal-clear understanding about what is and is not appropriate with respect to the use of various devices and online communication tools. To remind the child of this pledged commitment, we recommend that this contract be posted in a highly visible place at home. When there are violations, immediate logical consequences must be given that are proportionate to the misbehavior. Kids need to learn that inappropriate online actions will not be tolerated. Get them to understand that technology use and access is a privilege, and not a right and with those privileges comes certain responsibilities that must be respected. If a parent discovers that their child is cyberbullying others, they should first communicate how that behavior inflicts harm and causes pain in the real world as well as in cyberspace. We must remember that kids are not sociopaths, they are just kids who sometimes lack empathy and make mistakes. That said, there are ramifications for every choice they made. Depending on the level of seriousness of the incident and whether it seems that the child has realized the hurtful nature of his or her behavior, consequences should be firmly applied and escalated if the behavior continues. Moving forward, it is essential that parents pay even greater attention to the technology use of their child to make sure that they have internalized the lesson and are continually acting in responsible ways. Not only should they not be doing the wrong thing, they should be doing the right thing online!



What can youth do?

First and foremost, youth should develop a relationship with an adult they trust such as a parent, teacher, or someone else so they can talk about any experiences they have online and off that make them upset or uncomfortable. If possible teens should ignore minor teasing or name calling, and not respond to the aggressor as that might simply make the problem continue. If they can develop the ability to demonstrate resilience when targeted, it will bode well for their future since there will always be others who want to tear them down as they journey towards personal and professional success in life. Children should also use the account and privacy settings within each device, app, or network to control who can contact and interact with them, and who can read their online content. This can significantly reduce their victimization risk.

It's useful to keep all evidence of cyberbullying to show an adult who can help. If targets of cyberbullying are able to keep a log or a journal of the dates and times and instances of the online harassment, that can also help prove what was going on and who started it, which greatly helps during an investigation.

This information can also be forwarded to the respective site or company that serves as the venue or medium for the cyberbullying. Youth should take the time to report any harassment, threats, impersonation, or other problems they see or experience, and remember that their identity will be protected to the maximum extent of the law when doing so.

In addition, children should go online with their parents to show them what sites and apps they use, as well as share with them why they are great. Chat with them about what safety precautions they use while texting or tweeting, and tell them to give others a chance to come through for them if a problem arises.

Finally, they should pause before they post and make really wise decisions with what they share or send or post online, considering the possibility that anyone and everyone may see it including their parents, and others with opportunities to give them.

Protection from Harassment

Anyone who believes they are being harassed by another person can apply for a protection order at a magistrate's court under the Protection from Harassment Act. Includes Cyber harassment.

A child under the age of 18 can receive assistance without the child's parents.

For more information on the Protection from Harassment Act, 2011 (Act 17 of 2011):

http://www.justice.gov.za/forms/form_pha.html

LifeLine: Aims to cultivate and grow emotional wellness in individuals and communities:

[LifeLine - http://www.lifelinesa.co.za](http://www.lifelinesa.co.za)

The South African Depression and Anxiety Group: (SADAG) <http://www.sadag.org>



DON'T FALL VICTIM TO CYBERBULLYING

Learn what cyber bullying is and how you can help others .



QUICK TIPS

Check your privacy settings: they are there to help you manage your online experience in a positive way.

Disable unwanted location services: you don't really want the world to know where you live or play?

Think before you post: you can never permanently erase something that has been published on the internet.



GETTING HANDS ON



Bullying Tactics

- **Doxing:** to exact revenge, threaten or destroy the privacy of individuals by making their personal information public, including home address, phone numbers, links to social media accounts & other private data.
- Creating a webpage, posting comments, rumours, photos etc. about someone online that are mean, hurtful or embarrassing.
- Threatening to hurt someone or telling them to kill themselves.
- **Don't respond or encourage:** More often than not what your bully is looking for is some reaction from you. If you don't give them any, it's likely they'll leave you alone.
- **Don't retaliate:** If you retaliate, you are becoming a bully yourself! Remember, you only have control over how you react.
- **Save any evidence:** The one upside about cyberbullying is that it happens through technology, which means you can keep the evidence. If someone is sending you mean messages, screenshot them! You can bring them to an adult as proof!
- **Talk to a trusted adult:** You deserve backup. Adults are the best people to do that. If you experience bullying, talk to a parent! If you're not able to do that, talk to an adult at school, counselors will know how to handle your situation. Schools usually have a way you can anonymously report bullying if you're scared of people knowing you talked to someone.
- **Educate yourself:** The best way to stop cyber bullying is to recognize it when it starts. Educate yourself and your friends! Learn what cyber bullying is and how you can help others who are dealing with it.
- **Stay safe online:** Make sure you are the only one who has access to your passwords. Yes, even your best friend shouldn't have it! Make sure you log out of public computers as well. Be careful what you post, if it goes on the internet, it's accessible in some form forever, even if you think it's deleted! Finally, don't open messages or emails if you don't know the person who sent them. They could be inappropriate messages or even computer viruses!



WHY SHOULD I CARE?



PERSONAL



CHILDREN

Spot the warning signs: If your children start showing a change in behavior or mood, talk to them! It could be a sign of something more serious than you think. Avoiding group activities or events that they used to enjoy is another flag. Appearing anxious when receiving a text, image, or email.

Help educate your kids: Teach your children to stand up to bullying. If they see it happening online, show them that they can have a huge effect on that by speaking up. If they are going through it, teach them how to block the bully and explain the importance of deleting messages without reading them.

Personal Impact

- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Cyberbullies can take pictures of you by utilising your webcam / front camera.
- Cyberbullies can make audio and video recordings of you and your surroundings by making use of your devices.
- Cyberbullies can use these recordings and pictures for extortion.
- Accounts can be opened in your name without your knowledge.

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Cyberbullying can lead to depression, anxiety and suicidal behavior.
- Low self-esteem.
- Withdrawal from family and spending a lot of time alone.
- Reluctance to let parents or other family members anywhere near their mobiles, laptops etc.
- Finding excuses to stay away from school or work including school refusal.
- Friends disappearing or being excluded from social events.
- Losing weight or changing appearance to try and fit in.
- Fresh marks on the skin that could indicate self-harm and dressing differently such as wearing long sleeved clothes in the summer to hide any marks.
- A change in personality i.e. anger, depression, crying, withdrawn.





PHISHING

Definition:

Using fake websites to trick you into giving away personal information, “phishing” or “web spoofing” attacks use fraudulent websites to trick you into giving away confidential personal information such as credit card numbers, account usernames and passwords and ID numbers. This is called “phishing” because attackers are “fishing” for your personal information and trying to lure you into providing it.

A phishing attempt usually starts with an email urging you to click on a web link in order to check details about your bank account or another online account. These emails often appear to be from popular online institutions. When you click on the link you are directed to a page where you are asked for information. The page appears genuine, but is in fact counterfeit. Phishers may then use the personal information you have provided on the page to steal your identity or your money.

Phishing Email Scams

More than one-third of all security incidents start with phishing emails or malicious attachments sent to company employees.

Phishing scams continue to evolve and be a significant online threat for both users and organisations that could see their valuable data in the hands of malicious actors. The effects of phishing attacks can be daunting, so it is essential to stay safe and learn how to detect and prevent these attacks.

Phishing scams are based on communication made via email or on social networks. In many cases, cyber criminals will send users text messages/emails to try and trick them into providing valuable and sensitive data (login credentials – for their bank account, social network, work account or cloud storage account) that can prove to be valuable to them.

Moreover, these emails will seem to come from an official source (such as bank institutions or any other financial authority, legitimate companies or social networks representatives for users).

Attackers will use social engineering techniques by convincing you to click on a specific (and) malicious link and access a website which looks legit, but is actually controlled by them. You will be redirected to a fake login access page which resembles a real website. If you're not paying attention, you might end up providing the attackers with your login credentials and other personal information.

We've seen many spam email campaigns in which phishing was the main attack vector criminals used to spread financial and data stealing malware.

In order for their success rate to grow, scammers create a sense of urgency. They'll tell you a frightening story of how your bank account is under threat and how you really need to access, as soon as possible, a site where you must insert your credentials in order to confirm your identity or your account.

After you fill in your online banking credentials, cyber criminals use them to breach your real bank account or to sell them on the dark web to other interested parties.

What is Spear Phishing?

Spear phishing is an email or electronic communication scam targeted towards a specific individual, organisation or business. Although often intended to steal data for malicious purposes, cyber criminals may also intend to install malware on a targeted user's computer.

How it works: An email is received, apparently from a trustworthy source. The email then leads the unknowing recipient to a bogus website infected with malware. These emails often use clever tactics in order to attract the victims' attention. For example, the Federal Bureau of Investigation (FBI) has warned of spear phishing scams where the emails appeared to be from the National Center for Missing and Exploited Children.

In many instances, government-sponsored hackers and hacktivists are behind these attacks. Cyber criminals do the same with the intention to resell confidential data to governments and private companies. These cyber criminals employ individually designed approaches and social engineering techniques to effectively personalise messages and websites. As a result, even high-ranking targets within organisations, such as top executives, can find themselves opening emails they thought were safe. That slip-up enables cyber criminals to steal the data they need in order to attack networks.

How to Protect Yourself

Traditional security often doesn't stop these attacks because they are so cleverly customised. As a result, they're becoming more difficult to detect. One employee mistake can have serious consequences for businesses, governments and even non-profit organisations. With stolen data, fraudsters may reveal commercially sensitive information, manipulate stock prices or commit various acts of espionage. In addition, spear phishing attacks can deploy malware to hijack computers, organising them into enormous networks called botnets that can be used for denial of service attacks.



In order to fight spear phishing scams, individuals need to be aware of the threats, such as the possibility of bogus emails landing in their inbox. Besides education, technology which focuses on email security is necessary.

Above is an example of a sophisticated email scam making its rounds, that you should be very careful of.

See ahead for the related tips for your cyber survival.

USE YOUR PHISHING COMMON SENSE

If it looks too good to be true... it probably is.



QUICK TIPS



GETTING HANDS ON

Social engineering is when a cyber criminal manipulates a person psychologically, in order for that person to provide confidential information or to complete a task for them.

- Never share personal information, such as your ID number, on unverified websites or via email.
- Only engage people on social media you personally know, or referred by a trusted contact (verified).
- Limit personal information on your public social media accounts (for example don't make your Facebook home address publicly accessible).
- Review your privacy settings on your social media accounts.
- Be aware of who might be watching when entering pins and passwords.
- Use strong and unique passwords. The more complex the password the better.
- Do not enable GPS location tracking on social media i.e. don't allow social media sites or any other sites to automatically track your location.
- Do a background check (e.g. Google search) on people or companies before engaging with them.
- Disable other applications from accessing your Facebook account.

Avoid being scammed:

1. Do not click on links in emails, especially emails which appear to be from your bank.
2. Don't make hasty decisions. Think about the "opportunity" before proceeding.
3. Don't feel pressured to make an immediate decision even if the e-mail demands immediate action from you.
4. Always read any fine print very carefully.
5. Do not believe everything you read online or in emails.
6. Ask for more information on the person or company to verify the legitimacy.
7. Check the spelling of the content within emails and be sure to check the email address.
8. Cyber criminals often create new email addresses to scam people by merely adding a letter to the email address.

Don't become a victim of social engineering:

The following are some of the social engineering techniques used by cyber criminals.

- **Shoulder Surfing:** The attacker peers over your shoulder while you are typing in your pin or password.
Defence: Always be aware of who is around you and cover the keypad or keyboard when typing in your pin/password.
- **Dumpster Diving:** The attacker scavenges through dustbins for improperly disposed information which they can use against you or the organisation.
Defence: Never throw away confidential information in the dustbin - rather shred, burn or cut it into many pieces.
- **Baiting (Free USB):** The attacker leaves a USB where you are likely to find it, for example in the parking lot where you work, or hand them out for free at your local coffee shop. These USBs are usually loaded with what seems to be information you might be interested in, but instead contain viruses.
Defence: Never use USBs which were lying around or which are given out for free at untrusted places.



WHY SHOULD I CARE?



PERSONAL

Personal Impact

- Identity theft.
- Personal information theft.
- Your social media accounts can be compromised (hacked).
- You may suffer reputational damage, should hackers post unsavoury content obtained from hacked accounts.
- Your bank accounts could be compromised and money stolen.
- Your email account could be compromised (hacked) and used to send spam and scams to everyone in your address book.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings by making use of your devices.
- Criminals can use these recordings and pictures for extortion, blackmail or misrepresentation.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails spam.



CHILDREN

Children

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.



DEVICES

Device Security

- Criminals can implicate your devices in cybercrime.
- Your device can become infected with viruses or malware.



DATA

Data Security

- There are many incidents which could result in you losing some or all of your valuable data.



HELPFUL WEBSITES APPLICATIONS

- www.alertafrica.com
- For general awareness, news and to report a scam or cybercrime.
- www.scambuster.co.za/report-a-scam
- For reporting scams and getting news on the latest scams.
- <http://cybercrime.org.za/reporting>
- For reporting scams and getting news on the latest scams.
- <https://www.safps.org.za/index.aspx?ReturnUrl=/>
- To report Identity fraud/theft and how to protect your identity.



INSPECT LINKS BEFORE CLICKING

Banks will never request your password via email.



QUICK TIPS

- Banks will never ask you to send your password or supply other personal information in an email.
- If it sounds too good to be true it probably is - don't click on the link.



GETTING HANDS ON

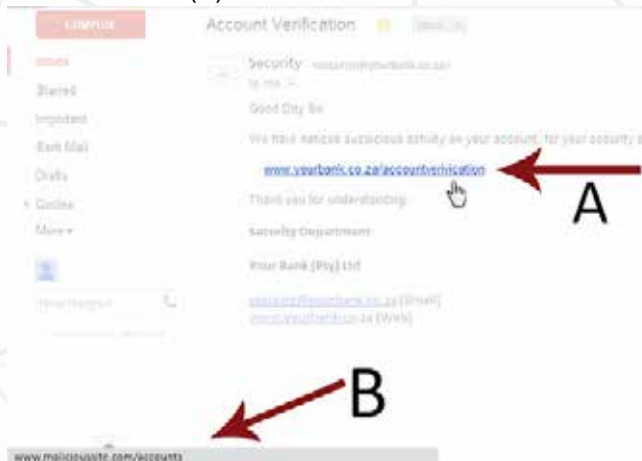


Determine if a link is malicious

- Copy the link (right-click, copy link – or highlight and press ctrl-C for PC).
- Go to www.virustotal.com.
- Click on the URL tab.
- Paste the link copied earlier.
- The result will show if the link is safe or not.
- Using VirusTotal is better than just clicking on the link, but it's important to remember that VirusTotal could indicate that a dangerous link is safe.
- If you have a bad feeling about the link - don't click it, even if VirusTotal says it's safe!

Inspect links (Hyperlinks)

- Look for obvious signs of tampering i.e. the sender email and web link are different (i.e. Sender: MyBank.com, Link: www.hackerbank.com).
- Hover your mouse pointer over the link (without clicking) then...
- (A) compare it to the link (B) in the bottom left hand corner:



Google and the Google logo are registered trademarks of Google Inc., used with permission.

Inspect short links (Compressed Links)

Periodically, you might encounter a short link or compressed link, such as: <http://is.gd/FZMBx2>

- When encountering a short link:
 - Go to <http://checkshorturl.com/>
 - Copy short link (right-click, copy link – or highlight, press ctrl-C for PC)
 - Paste it in at <http://checkshorturl.com/>
 - The full link will then be displayed and you can make your decision from there.



WHY SHOULD I CARE?



PERSONAL



CHILDREN



DEVICES



DATA

Clicking on a malicious link could result in you giving out personal information or your device getting infected with malware which could result in the following:

Personal Impact

- Identity and personal information theft.
- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Your bank accounts can be compromised (hacked).
- Access to email accounts, implicating them as set off points.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings by making use of your devices.
- Criminals can use these recordings and pictures for extortion.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails or used to spam your contacts.

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.

Device Security

- Criminals can implicate your device in cybercrime.
- Your device can become infected with viruses or malware.
- Your device can become very slow and sometimes even unresponsive.
- Your data usage will increase, resulting in high telephone bills.
- Slow Internet connection, due to the malicious applications sending and receiving data.

Data Security

- There are many incidents which could result in you losing some or all of your valuable data.



DON'T OPEN EMAILS OR ATTACHMENTS FROM UNTRUSTED SOURCES

Always be suspicious when opening emails and attachments.



QUICK TIPS

- Always be suspicious when opening emails and attachments.
- Business email accounts usually have a linked business-related domain (i.e. nameofbusiness.com) and not Gmail or Yahoo accounts. For example, abcBankSales@gmail.com would not be a legitimate email address for ABC Bank but sales@ABCBank.com would be.
- Banks will never send you emails requesting that you send your password via email or that you click on a link to reset your password.



GETTING HANDS ON



Spot a fake email

- Always be a little suspicious. "Guilty till proven innocent".
- The "From" field does not match the sender (the email is about your Facebook account, yet the "From" field indicates that the email was sent from a Gmail account).
- Obvious spelling and grammar mistakes.
- Other signs to look out for, if the email:
 - Is from a different country, (co.uk, .il etc.).
 - Asks for money, promising a reward in return, is very vague i.e. "Dear Sir/Madam" or "To whom it may concern".
 - Implies urgency ("Your account will be closed if you do not reset your password").
 - Requests personal information or requires you to reset your password by clicking on a link in the email.

Spot dangerous attachments

- Never open any attachments from unknown senders, especially those that have file names ending with the following:
- ".exe or .msi, .docm, .xlsm, .pptm, .zip, .rar".
- If you know the sender, ask about the file contents before opening.
- If your Antivirus flags it as dangerous, do not open it.
- For added safety, even if receiving an attachment from a known source, do the following:
 - Go to www.virustotal.com.
 - Click on "Choose File".
 - Choose the file you want to scan and click on "Ok".
 - Click on "Scan It!" The results of the scan will be shown, delete the file immediately if any antivirus product indicated that the file is a virus (malicious) i.e. the detection ratio is greater than 0.
- NOTE: Always click on "Reanalyse" if VirusTotal indicates that the file has already been analysed.



WHY SHOULD I CARE?



PERSONAL



CHILDREN



DEVICES



DATA

Clicking on a malicious link could result in you giving out personal information or your device getting infected with malware which could result in the following:

Personal Impact

- Identity and personal information theft.
- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Your bank accounts can be compromised (hacked).
- Access to email accounts, implicating them as set off points.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings by making use of your devices.
- Criminals can use these recordings and pictures for extortion.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails or used to spam your contacts.

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.

Device Security

- Criminals can implicate your device in cybercrime.
- Your device can become infected with viruses or malware.
- Your device can become very slow and sometimes even unresponsive.
- Your data usage will increase, resulting in high telephone bills.
- Slow Internet connection, due to the malicious applications sending and receiving data.

Data Security

- There are many incidents which could result in you losing some or all of your valuable data.





RANSOMWARE

Definition

Ransomware is a form of malware used by cyber criminals designed to block access to a computer system. A ransom fee is charged to decrypt/unblock the system/files.

Ransomware typically propagates like a conventional worm, entering a system through, for example, a downloaded file or a vulnerability in a network service. The program then restricts access to the computer system that it infects, and demands a ransom paid to the creator of the malware in order for the restriction to be removed. Some forms of ransomware encrypt files on the system's hard drive, while others may simply lock the system and display messages intended to coax the user into paying.

Ransomware goes beyond attempting to con its victims into handing over their money; it attempts to intimidate them. The extortion methods are expected to become harsher and more destructive.

Ransomware Prevention Methods

How to prevent a ransomware attack?

Back-up! Have a recovery system in place so that a ransomware infection can't destroy your personal data forever. It's best to create two to three back-up copies: one to be stored in the cloud (remember to use a service that creates an automatic backup of your files) and one to store physically (portable hard drive, thumb drive, extra laptop, etc.). Disconnect these from your computer when you are done. Your back up copies will also come in handy should you accidentally delete a critical file or experience a hard drive failure.

Use robust antivirus software to protect your system from ransomware. Do not switch off the 'heuristic functions' as these help the solution to catch samples of ransomware that have not yet been formally detected.

Keep all the software on your computer up-to-date. When your operating system (OS) or applications release a new version, install it. If the software offers the option of automatic updating, take it.

Trust no one. Literally. Any account can be compromised and malicious links can be sent from the accounts of friends on social media, colleagues or an online gaming partner. Never open attachments in emails from someone you don't know.

Cyber criminals often distribute fake email messages which look very much like email notifications from an online store, a bank, the police, a court or a tax collection agency, luring recipients into clicking on a malicious link and releasing the malware into their system.

Enable the 'Show file extensions' option in the Windows settings on your computer. This will make it much easier to spot potentially malicious files. Stay away from file extensions such as '.exe', '.vbs' and '.scr'. Scammers can use several extensions to disguise a malicious file as a video, photo, or document (like hot-chics.avi.exe or doc.scr).

If you discover a rogue or unknown process on your machine, disconnect it immediately from the internet or other network connections (such as home Wi-Fi) — this will prevent the infection from spreading.

If attacked, should I pay the ransom?

Paying the ransom is never recommended, mainly because it does not guarantee a solution to the problem. There are also a number of issues that can go wrong. For example, there could be bugs in the malware that makes the encrypted data unrecoverable even with the right key.

In addition, if the ransom is paid, it proves to the cyber criminals that ransomware is effective. As a result, cyber criminals will continue their activity and look for new ways to exploit systems that result in more infections and more money in their accounts.



Most ransomware attacks follow a typical mode of operation as explained below:

- Researching and identification of targets.
- Delivery of the initial exploit file through the appropriate infection vector.
- Once the initial exploit file has established persistence, a call is made to the command and control server to download the actual ransomware.
- Cryptographic parameters are set up, and then the encryption of files begin.
- Once encryption is complete, a ransom demand is made.

The following actions can be taken to either disrupt the attack or recover from it during the phases of the attack continuum:

Prior to attack:

- Delivery of end user security awareness education, to empower end users to be able to detect phishing emails and suspicious websites.
- Implementation of robust patch management practices on all systems including end user workstations.
- Hardening of all systems against security weaknesses.
- Comprehensive backup implementations – preferably what Veeam Software (<http://www.veeam.com>) refers to as 3-2-1 backup rule, which means, 3 copies of backup data, 2 different types of backup media and 1 offsite location.
- Making use of effective anti-malware solutions.
- Implementation of email gateway filtering to block emails with suspicious attachments.
- Implementation of proxy-based website filtering to block access to malicious website. Implementation of DNS filtering to identify malicious domains.
- Reduction of attack surface on endpoints by only installing required software and restricting network traffic flow.

During the attack:

Correlation of network event data from web / email gateways, anti-malware consoles, DNS/DHCP servers and other network nodes to enable timely detection of attacks. Preferably this should be accomplished through a Security Information and Event Management (SIEM) platform.

Acting on the security alerts being generated from the above.

After the attack:

- Containing the attack by isolating infected nodes.
- Disinfecting or re-imaging affected systems.
- Restore data from back-ups. Researching incident cause and remediating vulnerabilities to improve the security posture.
- Completing an incident report and any other actions as defined within the organisation's incident response plan.

Check the related tips provided for survival.



KEEP YOUR SOFTWARE UP-TO-DATE

Software updates very often contain critical security vulnerability fixes!



QUICK TIPS

- Activate automatic updates for all your software, including your Operating System (Windows), Antivirus, Adobe Reader, Adobe Flash and Java.
- Use helpful applications (listed below) to see if your other applications are up-to-date.



How to enable automatic updates for Windows 8.1

1. Open "Windows Update": With your mouse pointer move to the lower-right corner of the screen and moving the mouse pointer up, click "Settings", click "Change PC settings", and then click "Update and recovery".
2. Click "Choose how updates get installed".
3. Under "Important updates", choose "Install updates automatically".
4. Under "Recommended updates", select the "Give me recommended updates the same way I receive important updates" check box.
5. Under "Microsoft Update", select the "Give me updates for other Microsoft products when I update Windows" check box, and then click "Apply".



GETTING HANDS ON

How to enable automatic updates for Windows 10

1. Open "Windows Update Settings".
2. Using the Windows 10 search bar in the bottom left search "Windows Update Settings" and select the systems settings link that populates.
3. Select "Automatic Updates".
4. Once in "Windows Update Settings" select "Advanced Options".
5. Ensure that "Automatic" is selected in the drop down. You can now close the settings window.
6. Your Windows 10 will now update automatically.





WHY SHOULD I CARE?



PERSONAL



CHILDREN



DEVICES

If any of your devices are infected with viruses or malware , the following could happen:

Personal Impact

- Identity theft.
- Personal information theft.
- Your social media accounts can be compromised (hacked).
- You may suffer reputational damage should hackers post unsavoury content to hacked accounts.
- Your bank accounts could be compromised and money stolen.
- Email account compromised (hacked) and used to send spam and scams to everyone in your address book.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings using your device.
- Criminals can use these recordings and pictures for extortion, blackmail or misrepresentation.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails spam.

Children

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.

Device Security

- Criminals can implicate your device in a cybercrime.
- Your device can become infected with viruses or malware.
- Your device can become very slow and sometimes even unresponsive.
- Your data usage will increase, resulting in high telephone bills.
- Slow Internet connection, due to the malicious applications sending and receiving data.



HELPFUL WEBSITES/ APPLICATIONS

Commercial

- Ninite: <https://ninite.com/updater/>

Freely Available

- AppFresh: <https://www.techsupportalert.com/content/appfresh.htm-0>
- Secunia PSI: <https://www.flexera.com/products/software-vulnerability-management>
- SUMo: <http://www.kcsoftwares.com/index.php?sumo>
- Update Checker: <http://filehippo.com/updatechecker>



INSTALL ANTIVIRUS ON ALL DEVICES

Do not install more than one antivirus per device!



QUICK TIPS

- Download and install either a commercial or a free antivirus.



GETTING HANDS ON



WHY SHOULD I CARE?



PERSONAL



CHILDREN

Choose an antivirus solution.

- Free solutions work but often don't have the added features of commercial versions.
- The easiest way for more comprehensive protection is choosing an antivirus suite. These suites are normally called "Internet Security".
- Reasons to choose an Internet Security Solution (antivirus suite) over an antivirus solution are:
- In addition to an antivirus, Internet Security suites normally include the following tools:
 - Firewall
 - Parental control
 - Anti-Spam.
- Before paying for an antivirus suite solution use the trial version for 30 days and see if you like it. Remember don't install more than one antivirus and Internet Security suite.

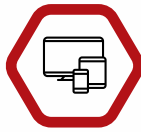
If any of your devices are infected with viruses or malware, the following could happen:

Personal Impact

- Identity and personal information theft.
- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Your bank accounts can be compromised (hacked).
- Access to email accounts, implicating them as set off points.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings using your device.
- Criminals can use these recordings and pictures for extortion.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails or used to spam your contacts.

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.



DEVICES

Device Security

- Criminals can implicate your device in cybercrime.
- Your device can become infected with viruses or malware.
- Your device can become very slow and sometimes even unresponsive.
- Your data usage will increase, resulting in high telephone bills.
- Slow Internet connection, due to the malicious applications sending and receiving data.



DATA

Data Security

- There are many incidents which could result in you losing some or all of your valuable data.



HELPFUL WEBSITES/ APPLICATIONS

Commercial

- Bitdefender: <https://www.bitdefender.com/solutions/internet-security.html>
- ESET: <http://www.eset.co.za/za/home/>
- Kaspersky: <https://www.kaspersky.co.za/internet-security>

Freely Available

- All three options listed offer commercial versions, with added features.
- Avast: <http://www.avast.com>
- Avira: <https://www.avira.com/en/avira-free-antivirus>
- Bitdefender: <http://www.bitdefender.com/toolbox/freeapps/desktop/>

Solutions offered by Banks:

- Absa - Antivirus Software (Trend Micro Maximum Security 2017 11.0)
 - (<https://www.absa.co.za/security-centre/tips-and-tools/antivirus-software/>)
- FNB - Trend Micro™
 - (<https://www.fnb.co.za/security-centre/security-software/trend-mirco.html>)
- Nedbank – Trusteer Rapport
 - (<https://www.nedbank.co.za/content/nedbank/desktop/gt/en/personal/tools-and-guidance/bank-anytime-anywhere/trusteer-rapport-security.html>)
- Standard Bank - Trustee
 - (https://www.standardbank.co.za/static_file/South%20Africa/PDF/Miscellaneous/Trusteer%20Rapport_security.pdf)

Note: This is not a comprehensive list of all software solutions.

Free Online Scanning:

- Go to www.virustotal.com
- Click on “Choose File”
- Choose the file you want to scan and click on “Ok”
- Click on “Scan It!”
- The results of the scan will be shown, delete the file immediately if any antivirus product indicated the file is a virus (malicious) i.e. the detection ratio is greater than 0.

Note: Always click on “Reanalyse” if VirusTotal indicates that the file has already been analysed.



REVIEW APP PERMISSIONS BEFORE INSTALLING AN APPLICATION

Do the permissions requested by the app make sense?



QUICK TIPS

- Read app permissions before accepting or installing the app.
- Do the permissions requested by the app make sense? For example, a weather app should not have access to your contact list.
- Only install apps from trusted sources (Google Play Store, iTunes Store etc.)
- Do not Jailbreak (Apple) or Root (Android) your device.



GETTING HANDS ON



Before installation

- Read through the permission requests and see if they make sense (i.e. the app requests to access contacts but the app is used to view images).

After installation

- Use apps like "App Permissions" to review permissions other apps have.
- As you review these permissions, think about what the app does and if the permissions it has fits its use.



HELPFUL WEBSITES/ APPLICATIONS

Commercial

- NOTE: Disabling app permissions can cause apps to stop working properly (crash), thus these apps are recommended for use by advanced users ONLY.
- Adv Permission Manager (Pro)
- Permission Manager Pro
- Permissions Viewer

Freely Available

- These apps allow you to view the permissions of the other apps installed on your device. They do not disable any permissions and can be used without worrying that you might break something.
- App Permissions
- Clueful
- Permission Manager - App ops



WHY SHOULD I CARE?



PERSONAL

Clicking on a malicious links could result in you giving out personal information or your device getting infected with malware which could result in the following:

Personal Impact

- Identity and personal information theft.
- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Your bank accounts can be compromised (hacked).
- Access to email accounts, implicating them as set off points.



PERSONAL

- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings using your device.
- Criminals can use these recordings and pictures for extortion.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails or used to spam your contacts.



CHILDREN

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.
- Untrusted people can track the movements of your family from geotags in certain pictures posted on the web.
- Untrusted people (e.g. paedophiles) can gather intelligence on your family from various online sources and attempt to contact your children.



DEVICES

Device Security

- Criminals can implicate your device in cybercrime.
- Your device can become infected with viruses or malware.
- Your device can become very slow and sometimes even unresponsive.
- Your data usage will increase, resulting in high telephone bills.
- Slow Internet connection, due to the malicious applications sending and receiving data.



DATA

Data Security

- There are many incidents which could result in you losing some or all of your valuable data.



PROTECT YOUR DATA

Back-up and protect your valuable data.



QUICK TIPS

- Back-up your most valuable information first (e.g. documents, family pictures).
- Do not keep your back up drive ("external hard drive") close to your computer when you are not using it.
- Encrypt your hard drive.
- Back-up valuable information to reputable cloud storage providers (e.g. Dropbox).
- Shred or cut:
 - Paper documents that may contain personal information.
 - Old credit and loyalty cards.
 - CDs that may contain personal information.
- Delete emails that contain personal information.
- Remember to "Empty" the Recycle Bin (Windows) or Trash (Mac).
- Password protect ALL your devices.



GETTING HANDS ON



Manually Creating a Backup

Things you'll need:

- Storage media (e.g. External Hard drives, DVDs, USBs).
- Select the files to back-up (Documents, Pictures, Music and Videos).
- Copy the selected files to your Storage Media.

Automatically Creating a Backup

Things you'll need:

- Storage media (e.g. External hard drives, DVDs, USBs).
- Open the backup program of your choice (some examples given below).
- Follow instructions or prompts.
- NOTE: Do not store your back-up on the same device that you need to back-up.

Distribute back-ups

- Don't keep back up drives in your laptop bag or next to your computer.
- Back-up critical (most valued) information to trusted Cloud services like Dropbox or Google Drive.
- Duplicate critical backups to USBs or DVDs and store safely elsewhere.

Permanently dispose of paper documents

- Shred unwanted physical documents.

Empty the "Recycle Bin"

- Right click on the Recycle Bin icon (image).
- Choose "Empty Recycle Bin".

Properly Dispose of Hard drives you no longer need

- Physically destroy the hard drive (For example, with a hammer).
- Wipe a hard drive (Formatting does not always wipe a drive).

Password Protect Devices

- For instructions on how to set a password for Windows visit <http://windows.support.microsoft.com/en-us/help/14087/windows-7-change-your-windows-password>

Set a lock pattern or pin on your mobile devices (including your phones). This can be typically set on the mobile device's settings menu under security settings.



HELPFUL WEBSITES/ APPLICATIONS

BACK-UP APPLICATIONS:

Commercial

🍏 Carbon Copy Cloner:

http://sites.fastspring.com/bombich/product/cccl?option=show_contents

🖥️ Genie Backup Manager 9:

http://www.genie9.com/home/genie_backup_manager_home/Overview.aspx

🖥️ Nova BACKUP Professional 15:

<http://www.novastor.com/en/release/15>

Freely Available

🖥️ AOMEI Backupper: <http://www.aomeitech.com/>

🖥️ EaseUS Todo Backup:

<http://www.todo-backup.com/products/home/free-backup-software.htm>

🖥️ FBackup: <http://www.fbackup.com/>

🍏 Time Machine (Installed on Mac)

CLOUD STORAGE:

Commercial

🖥️ 🍏 🤖 SugarSync: <https://www2.sugarsync.com/>

The service providers below offer an initial quota of free storage, with additional space available on subscription basis

🖥️ 🍏 🤖 Dropbox: <https://www.dropbox.com/> (2GB Storage Free)

🖥️ 🍏 🤖 Google Drive: <https://drive.google.com/> (15GB Storage Free)

(If you have a Gmail account you already have Google Drive)

🖥️ 🍏 🤖 Microsoft One Drive : <https://onedrive.live.com/about/en-us/>

(7GB Storage Free) (Can link to your Microsoft account if you have one, if not signing up will create one)

🖥️ 🍏 🤖 Spider Oak: <https://spideroak.com/> (2GB Storage Free)

(Spider Oak Encrypts your data on the fly to ensure your privacy)



WHY SHOULD I CARE?



PERSONAL

The following can happen if you do not adequately protect your data on all your devices:

Personal Impact

All your personal information can be stolen and misused as follows:

- Your identity can be stolen.
- Your personal information can be stolen.
- Your social media accounts (Facebook, Twitter etc.) can be compromised.
- You may suffer reputational damage should hackers post unsavoury content on hacked accounts.
- Your bank accounts could be compromised and money stolen.
- Criminals may gain access to all information in your email accounts. They may also attempt to illicit further information or money from your contacts.
- You could fall for scams that end up costing you money or endanger your family.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails (spam).



DATA

Data Security

- Devices which get stolen or misplaced risk having their data compromised.
- There are many incidents which could result in you losing some or all of your valuable data.



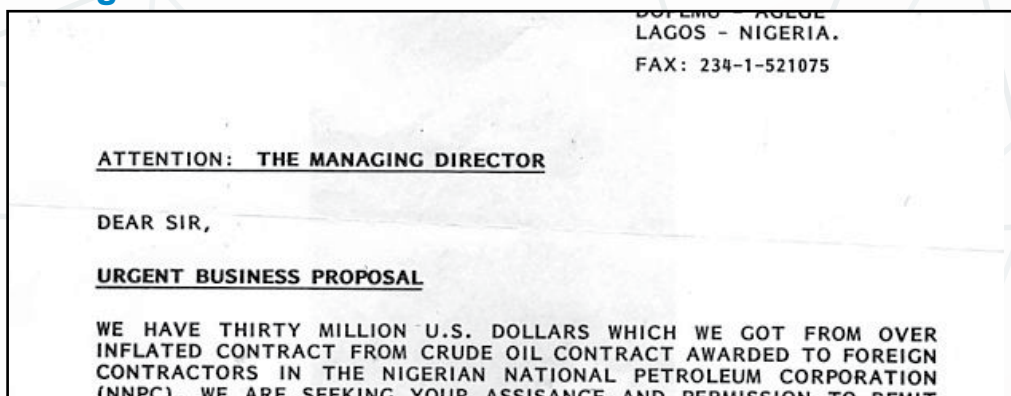


01 Phishing Scams



In most cases phishing emails are sent to try and trick the intended victim into visiting a fraudulent website disguised to look like a valid eCommerce or banking site. Victims think they are logging into their actual account, but instead, everything they enter on the fake site is being sent to the scammers. Armed with this information, the scammer can wipe out the victim's accounts, run up their credit cards, or even steal their identity.

02 Nigerian 419 Scams



Nigerian 419 scams (aka Advanced Fee Fraud) date back to the days when fax machines and snail mail were the primary business communication tools. Today, email is the preferred method of these scammers and there are more Nigerian 419 Advanced Fee Fraud scams and victims than ever before.

03 Greeting Card Scams



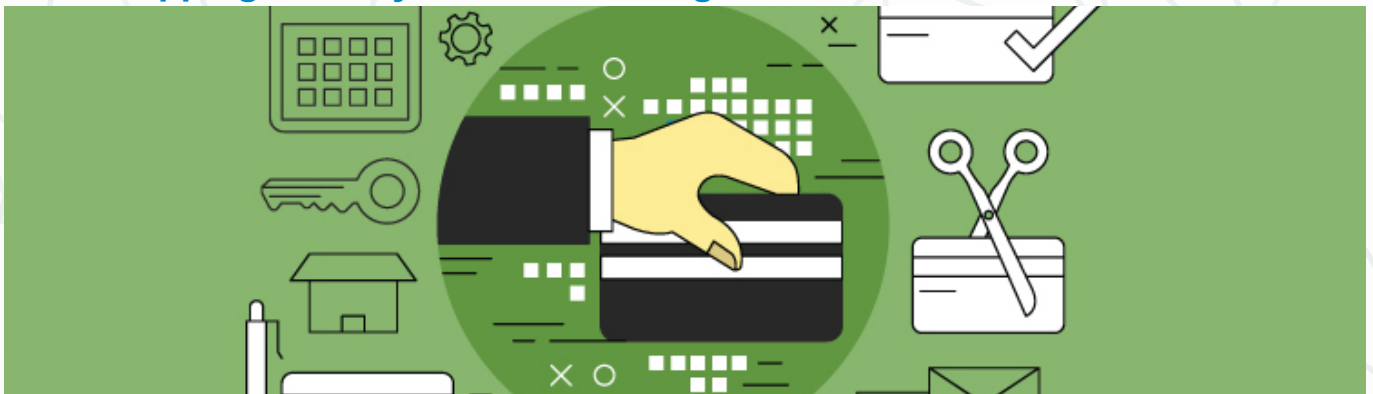
Greeting card scams arrive in email pretending to be from a friend or family member. Clicking the link to view the card typically leads to a booby-trapped web page that downloads Trojans and other malicious software onto the systems of the unsuspecting victim.

04 Sextortion Scam



The practice of forcing someone to do something, in some cases, to perform sexual acts, by threatening to publish naked pictures of them or sexual information about them. The number of victims is unknown. Many are too embarrassed to report sextortion. Cyber criminals are increasingly making use of Sextortion to target individuals.

05 Reshipping and Payment Processing Fraud



The ad should read: Help Wanted to illegally launder money on behalf of criminals. However, it doesn't. Instead, it couches the crime in soft terms like 'payment processing' and 'reshipping transactions.' Don't be fooled - victims not only find themselves engaged in illegal activity, but they will also be on the legal hook for the entire amount transferred and any fees that result.

06 Lottery Winning Scams



Lottery winner scams attempt to trick recipients into believing they have won large sums of cash, and then bilks them out of their own money in a similar fashion to the Nigerian 419 scam.

07 Pump and Dump Stock Scams



Pump and dump scams send large volumes of emails which pretend to disclose confidential information about a particular stock in an attempt to inflate the price.

08 Fraudulent Link Scams



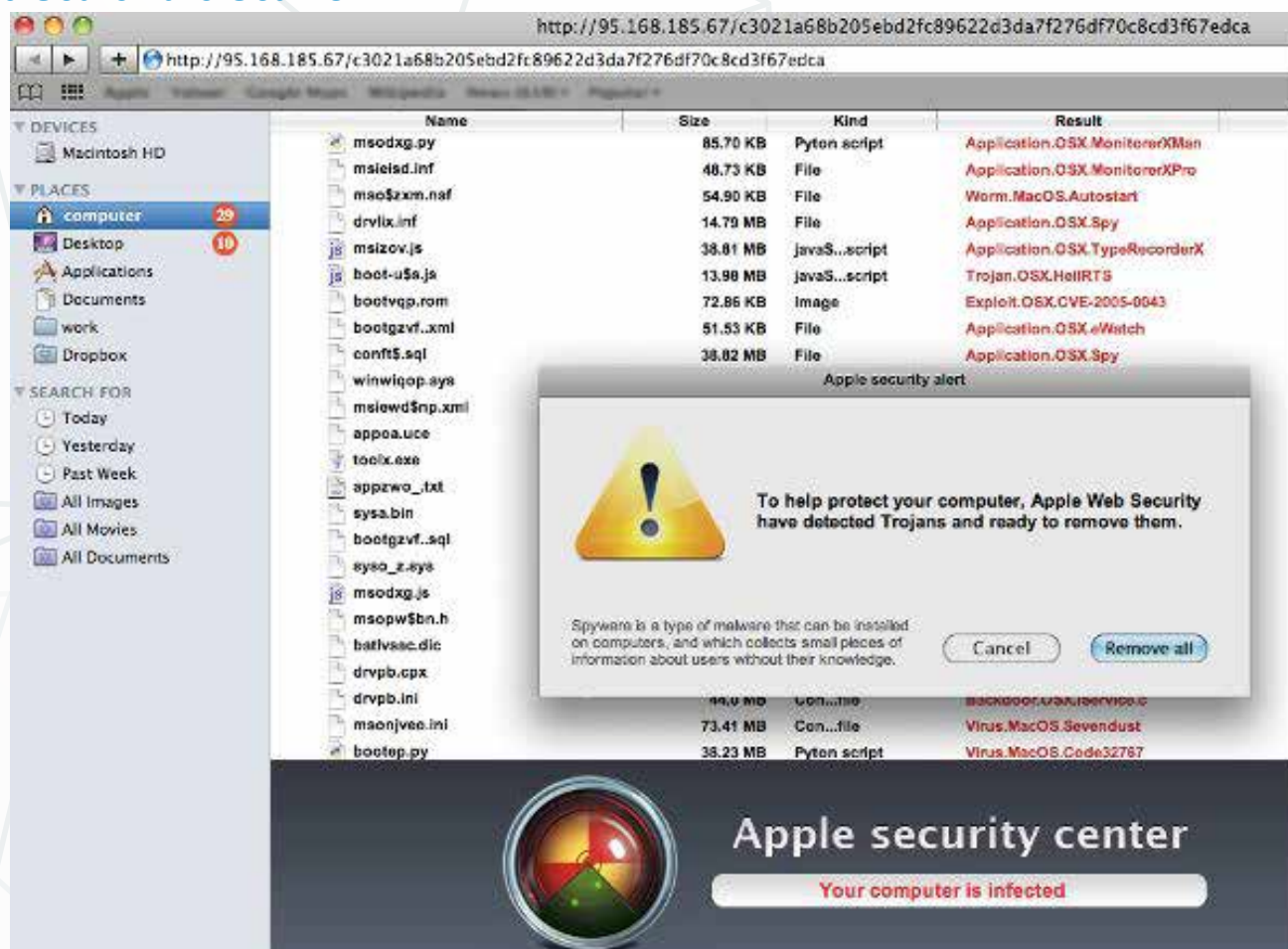
Scams, in general, are the new malware delivery method. Social engineering is the norm. Falsifying a link is the hallmark of phishing scams, seeded downloader Trojans, and other web-based malware. It is all trivially easy to do, using basic HTML.

09 Killer Spam: Hitman Email Threatens Recipients



Imagine opening your email inbox and reading a message from an alleged assassin claiming you're the target. It sounds like something out of a horror movie, but it's been happening in real life to hundreds of people. The gist of the email is pay the hitman thousands of dollars or die.

10 Scareware Scams



Scareware erroneously claims the system is infected and instructs the user to purchase a 'full version' in order to clean the bogus infections. Sometimes, fake antivirus software gets installed by the user who fell victim to an advertising scam. Other times, a rogue antispyware scanner may be installed by exploit, a so-called 'drive-by install.' Regardless of how the rogue software gets installed, the user is often left with a hijacked, crippled system. To avoid becoming a victim, before installing any software on the Internet, search for the name of the product online. Don't skip this step and you'll go a long way towards a safer online experience.

CREATE STRONG AND UNIQUE PASSWORDS

Enable passwords on all your devices: laptops, mobile phones and tablets.



QUICK TIPS

Enable passwords on all your devices.

- Ensure passwords are longer than 7 characters.
- Use a combination of numbers and special characters (e.g. @ # \$ % ! ?).
- Use different passwords for all your different accounts and devices.
- Do not share your password with anyone.
- Never write your password down.



GETTING HANDS ON



Avoid weak passwords

Do not use passwords similar to the following:

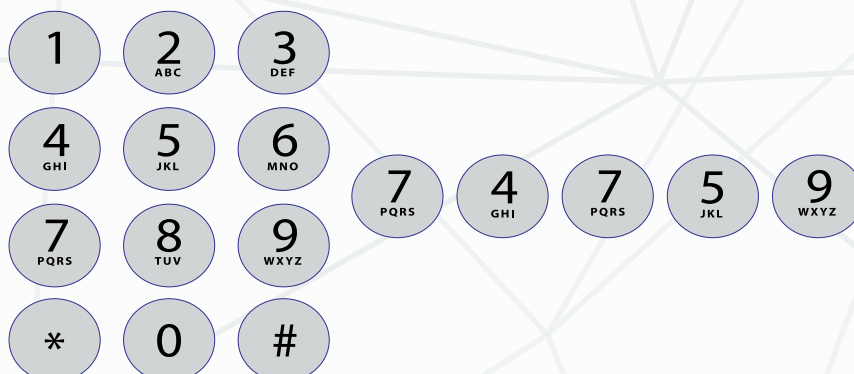
- "123456"
- "password"
- "qwerty"
- "iloveyou"
- Do not use dictionary words i.e. single words out of a dictionary.
- Do not include personal references in your password (date of birth, pet names).

Manually creating a strong password

- Minimum length of 7 characters.
- Use spaces or a combinations of:
- Upper case and lower case letters.
- Numbers.
- Special characters (e.g. @ # \$ % ! ? . -).
- Example: "r4XSVY_/" *Do not use this example.
- Use a pas1sphrase and add special characters and numbers to it.
- Example 1: Take the phrase "Online banking saves me so much time and effort every day" and then use numbers and letters to recreate it:
- Password "Obsmsmt&eed!2014" The password was created by using the first letter of each word. *Do not use this example.

Remember PIN's

- Spell a word using the keyboard/keypad.
- Example: Risky -> 74759 *Do not use this example.





WHY SHOULD I CARE?



PERSONAL

Using a weak password may result in the following:

Personal Impact

- Your identity can be stolen.
- Your personal information can be stolen.
- Your social media accounts (Facebook, Twitter) etc, can be compromised.
- You may suffer reputational damage should hackers post unsavoury content on hacked accounts.
- Your bank accounts could be compromised and money stolen.
- Criminals may gain access to all information in your email accounts. They may also attempt to illicit further information or money from your contacts.



HELPFUL WEBSITES/ APPLICATIONS

Commercial

- The following applications can be used to automatically generate secure passwords for each service that you use. The applications typically require that you set one master password that must be entered to unlock the "vault" storing all the other passwords. Ensure you set a strong master password according to the guidelines provided in the previous section.
- 1Password: <https://agilebits.com/onepassword>
- F-Secure Key: http://www.f-secure.com/en/web/home_global/key
- Password Manager: <http://www.kaspersky.com/password-manager>

Freely Available

- Identity Safe: <https://identitysafe.norton.com/>
- Last Pass: <https://www.lastpass.com/>
- KeePass : <http://keepass.info/download.html>



LOG OFF

Do NOT check, 'Keep Me Logged In' or 'Remember Me'



QUICK TIPS

- Do NOT check 'Keep Me Logged In' or 'Remember Me', especially on public computers!



GETTING HANDS ON



Logging in automatically

- When logging into your account ensure that the "Keep Me Logged" In or "Remember Me" check box is NOT checked.
- If your browser (Internet Explorer etc.) prompts you to "Remember user name and password" decline the request (Say no).

Log out

- When you are finished with your emails or social media, click the "Log Out" or "Sign Out" button / link. It is normally in the top right hand corner of the webpage.



WHY SHOULD I CARE?



PERSONAL

Personal Impact

- Your identity can be stolen.
- Your personal information can be stolen.
- Your social media accounts (Facebook, Twitter etc) can be compromised.
- You may suffer reputational damage should hackers post unsavoury content on hacked accounts.
- Your bank accounts could be compromised and money stolen.
- Criminals may gain access to all information in your email accounts. They may also attempt to illicit further information or money from your contacts.



HELPFUL WEBSITES/ APPLICATIONS

Password managers (as mentioned in CST 7, Helpful Applications), can centralise and automate your logins across multiple websites with one central "Master" password - which is safer than staying logged into accounts when idle or not used.

BE CAUTIOUS WHEN USING BLUETOOTH AND WI-FI

Only turn on Wi-Fi and Bluetooth when you need it.



QUICK TIPS

- Do not connect to "Free" (open) Wi-Fi networks that public stores offer.
- Do not accept unknown Bluetooth pairing requests.
- Secure your Wi-Fi at home.



GETTING HANDS ON



WHY SHOULD I CARE?



PERSONAL



CHILDREN



DEVICES

Safely use Free (open) Wi-Fi

- Using a VPN is the safest way to use free Wi-Fi. However, setting up and using a VPN is beyond the scope of this guide.
- Do not bank, shop online, or surf social media sites using free Wi-Fi networks.
- Always ensure you are using a secure connection (https rather than http).
- Simply look for the padlock icon (🔒)



Personal Impact

- Identity and personal information theft.
- Social media account breach.
- Reputational damage, extortion and blackmail due to hacked accounts.
- Your bank accounts can be compromised (hacked).
- Access to email accounts, implicating them as set off points.
- Criminals can take pictures of you by utilising your webcam / front camera.
- Criminals can make audio and video recordings of you and your surroundings using your device and use these recordings and pictures for extortion.
- Your credit record can be damaged.
- Accounts can be opened in your name without your knowledge.
- Your email inbox could be flooded with unwanted emails or used to spam your contacts.

Child Safety

- Images of you or your family can be harvested without your permission and used on unsavoury websites.

Device Security

- Criminals can implicate your device in cybercrime.
- Your device can become infected with viruses or malware.

WHERE TO APPLY THE CYBERCRIME SURVIVAL TIPS

Online Banking, Shopping and Social Media:

Cybercrime Survival Tips:

- Use your common sense
- Keep your software up-to-date
- Install antivirus on all devices
- Inspect links before clicking
- Don't open email or attachments from untrusted sources
- Review app permissions before installing an application
- Create strong and unique passwords
- Log off
- Be cautious when using Bluetooth and Wi-Fi

General Tips:

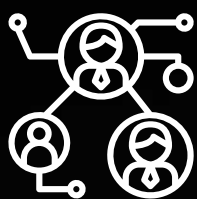
Type the address yourself

- Always type out the address (URL) of your bank i.e. www.yourbank.co.za

Secure Connection

- Ensure that you have a secure connection: https over http.
- Look for the lock icon (🔒)





STAYING SAFE ON SOCIAL MEDIA



How to keep your account secure?

Implement the above mentioned CSTs to keep your account secure

Built in Security Features.

Facebook has a range of security features users can activate to better protect their account.

Facebook features:

- Login approvals (Two-Factor Authentication)
- Login notifications
- One time passwords
- Trusted contacts

For more information on these Facebook security features go to:

<https://www.facebook.com/security>

Twitter has security features users can activate to help protect their account.

Twitter features:

- Login verification (Two-Factor Authentication)
For more information on keeping Twitter safe go to: <https://help.twitter.com/>

Gmail has security features users can activate to help protect their account.

Gmail features:

Two-Factor Authentication
For more information on Two-Factor Authentication go to:

<https://www.google.com/landing/2step/>





How do you know if your account has been hacked?

You cannot access your account with your normal login credentials.

There are posts on your news feed that you never posted.

These posts encourage your friends to click on the links.

You cannot access your account with your normal login credentials.

There are Tweets from your account that you didn't personally make.

You cannot access your account with your normal login credentials.

People receive emails from you that you didn't send.

What to do if your account has been hacked.

Clean your computer from malicious software before changing your password
Scan your computer for any malicious software and make sure your antivirus is up-to-date. Do not change your password until you are certain the computer you are using is free of all malicious software.

Change your password.

If you still have access to your account change your password (have a look at password management).

If you do not have access to your account, reset your password by clicking on the "Forgot your password" link on the log in page.

Clean your computer from malicious software before changing your password
Scan your computer for any malicious software and make sure your antivirus is up-to-date.

Do not change your password until you are certain the computer you are using is free of all malicious software.

Change your password.

If you still have access to your account change your password (have a look at password management).

Clean your computer from malicious software before changing your password
Scan your computer for any malicious software and make sure your antivirus is up-to-date.

Do not change your password until you are certain the computer you are using is free of all malicious software.

Change your password.

If you still have access to your account change your password (have a look at password management).





Remove any third-party applications that you installed on Facebook
Report a compromised account.

- Go to <https://www.facebook.com/help/hacked>
- Notify friends
- After getting back control of your account, notify all your friends that your account was hacked and that any suspicious posts are as a result of the hack.

<https://www.facebook.com/help/hacked>



If you do not have access to your account, reset your password by clicking on the "Forgot your password" link on the log in page.

Notify followers, notify all your friends that your account has been hacked and that any suspicious tweets are as a result of the hack.

<https://support.twitter.com>
->Troubleshooting



If you do not have access to your account, reset your password by clicking on the Forgot your password link on the log in page.

After taking back your account, notify all your contacts that your account has been hacked and that any suspicious emails they received are as a result of the hack.

<https://support.google.com/mail#topic=7065107>

What to do if your account has been hacked?

More Information.



Glossary



Glossary contains explanations of concepts. In this sense, the term is related to the notion of ontology that transform a glossary into an ontology.

419 Scam

Claim that your help is needed to access a large sum of money, usually millions of dollars. When in fact the money does not exist. Attempt to trick people into believing that they had a wealthy uncle or aunt from overseas who has left a fortune that needs to be claimed by a person with the same surname.

Adware

Malicious software that allows unwanted advertisements on your computer.

Antivirus

Software designed to protect your computer from harmful software (Malware, Viruses, Trojan, etc.).

Charity scam

Swindling of money by scammers in the guise of a worthy cause. Victims are asked to donate for a 'special cause'. But the charity turns out to be a fraud, or a scammer pretending to be a real charity.

Classified scam

Scammers enjoy tricking people into purchasing non-existent or sub-standard goods online. Scammers are not always on the selling side but also act as interested parties (clients).

Employment scam

Employment scams are conducted by unscrupulous people that pose as employers. The scammers may ask you to pay a recruitment administration fee to assist you in getting a job or will ask for money for visa processing or travel expenses.

Encryption

Computer algorithms that encode your data, making it unreadable unless you have the correct password.

Government grant scam

Usually advertisements, claiming that you qualify for a 'free' grant to pay for housing or education costs. Perpetrators may pose as a 'government' or an organisation with official name. The claim is always that your application for a grant is accepted, that you will never have to pay back the money.

Investment scam

Includes investment opportunities and expert tip-offs on rising shares. Deals often sound tempting, resulting in victims losing large sums of money.

Key logger

Malicious software or device that captures everything you type. Criminals can use this to get your password.



Lottery scam

Proceeds hardly go towards the cause and when they do, it is usually just a fraction of the proceeds. Lottery and competition scams also come in varied forms, via email, texts, or through social media and is often a lottery or competition that you did not enter.

Malware

Is used to describe all the malicious software like Viruses, Trojans and Worms. The term Virus is often wrongly used to describe all malicious software, the correct term is malware.

Phishing

When criminals pursue sensitive information about you like usernames, passwords and ID numbers.

Ransomware

Malicious software that locks (encrypts) the computer it infects, and demands payment to unlock (decrypt) it. Remote access tools (RATs) Malicious software used to control your computer remotely.

Rootkit

Malicious software used to control your computer. Spyware is malicious software that monitors computer activities without the user's knowledge, and the intent to get private information.

Telemarketing scam

Targets of this type of fraud are usually those aged 60-upwards, coerced to buy bogus products offerings by telephone including free prizes, low-cost vitamins and healthcare products and vacations.

Traveling/Holiday scam

Unsuspecting victims are targeted by fraudulent holiday/travel tour agents - offered a tempting holiday at a fraction of normal cost. Even though there are genuine holiday discounts it is important to research holiday vouchers, booking accommodation online, or sorting out a visa for your trip.

Trojan

Malicious software hidden in a normal application or software that claims to be legitimate.

Operating System

The software that manages your computer and operation. (Windows, Mac OS X and Linux).

Virus

Malicious software created with intent to harm your computer or to be used for cybercrime. The term virus is often confused with malware.

Worm

Malicious software that can spread itself on computers without user's interaction. Once a virus is able to do this it is now classified as a worm.



SOURCES

Cyberbullying

<https://cyberbullying.org/what-is-cyberbullying>

http://www.scielo.org.za/scielo.php?script=sci_arttext&pid=S0256-01002015000200001

<https://www.connectsafely.org/tips-to-help-stop-cyberbullying/>

Phishing

<https://www.kaspersky.co.za/resource-center/definitions/spear-phishing>

Ransomware

<https://www.nomoreransom.org/en/index.html>

General

<http://cybercrime.org.za/>

Online Scams

<https://heimdalsecurity.com/blog/top-online-scams/>

Online Banking Scams

<https://www.sabrics.co.za/stay-safe/>



**LET US NOT LOOK
BACK IN ANGER
OR FORWARD
IN FEAR
BUT AROUND
IN AWARENESS**



WOLVES ALWAYS HUNT IN A PACK



In order to manage IT governance, privacy and information security risks effectively, you need great people on your team.

Wolfpack specialises in business-aligned information risk and cyber threat management. We cover the full spectrum of prevention, detection and resilience requirements.

The Wolfpack portfolio includes:

Advisory

Awareness

Managed Services

Training



PROTECTION IN THE PACK

Contact: info@wolfpackrisk.com or visit: www.wolfpackrisk.com

[illegible]

