WILMINGTON TRUST

MEMBER OF THE M&T FAMILY

Cybersecurity Threats and What to Look for

Ransomware

DEFINITION:
Use of malicious software (malware) that, when downloaded to a computer, encrypts files or locks system down so they can no longer be accessed.

WATCH FOR:

- **Requests from unknown entities to remotely access your system**
- **Links to download software to your system from unfamiliar contacts**

40% **of ransomware incidents use of Desktop sharing software**

35% **involved the use of email**[1]

Credential reuse

DEFINITION:
A trend where people re-use the same username and password on multiple sites.

Threat actors can obtain username and password combinations from various breaches and log-in using the stolen credentials to see ultimately commit fraud or sell the information.

WATCH FOR:

- **Utilization of the same or similar passwords across multiple sites**

33% **create stronger passwords for their work accounts**

50% **never change their password after a breach**[2]

Social engineering

DEFINITION:
Use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

WATCH FOR:

- **Emails that look to be from a familiar source but are asking to provide personal information**
- **Emails with a sense of urgency or exploitation of seasonal opportunities**

- **Masquerading as some-one you may know**
- **Containing a download**
- **Containing a link**
- **Asking for urgent assistance**

Continued

Phishing

DEFINITION:
Use of a fraudulent email to trick the recipient into opening a malicious attachment or website.

The goal is to have you divulge sensitive information or provide an avenue for the hacker to steal your credentials.

WATCH FOR:

- **Emails from unknown or unfamiliar sources asking you to open attachments or links**
- **Usually have a sense of urgency or exploitation of seasonal opportunities**

1 in 25

branded emails are actually phishing attempts[3]

Synthetic identities

DEFINITION:
A combination of fabricated credentials where the implied identity is not associated with a real person.

WATCH FOR:

- **Being contacted about an account you did not open**
- **Aliases appearing on your credit report or dramatic lowering of your credit score**

An estimated **40%** of identified synthetic identities were constructed using information stolen from children born after 2011, according to a recent white paper from GIACT, a leading fraud prevention company.[4]

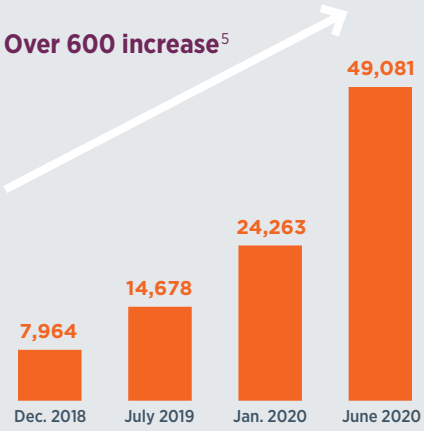
Deepfake

DEFINITION:
Refers to a video that has been edited using an algorithm to replace the person in the original video with someone else (especially a public figure) in a way that makes the video look authentic.

WATCH FOR:

- **This is a more difficult threat to detect due to the growing sophistication of the technology used**

Over 600 increase[5]



Continued

Never share passwords, login credential, or any authentication information.

Always use a SPAM filter, anti-virus software, and a personal firewall.

We hope you found this information to be valuable.

Talk to us about how we can assist with your corporate and institutional business ventures.

Visit https://www.wilmingtontrust.com/corporate-institutional

FOOTNOTES:

[1] Source: 2022 Verizon Data Breach Investigations Report.

[2] Source: LastPass, survey of 3,750 professionals, November 2022. www.lastpass.com/resources/ebook/psychology-of-passwords-2022

[3] Source: https://www.thesslstore.com/blog/20-phishing-statistics-to-keep-you-from-getting-hooked-in-2019/

[4] Sources: https://www.paymentsjournal.com/synthetic-identity-fraud-is-rising-giacts-fighting-back/
https://www.idanalytics.com/solutions-services/fraud-risk-management/synthetic-identity-fraud/

[5] Sources: https://www.theverge.com/2020/7/27/21339898/deepfake-audio-voice-clone-scam-attempt-nisos