



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 email¹

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 breach²

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 someone you may know**
- **Containing a download**
- **Containing a link**
- **Asking for urgent assistance**



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 attempts³



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

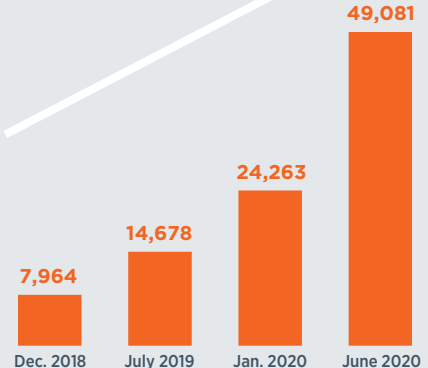
DEFINITION:

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 increase⁵



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.thesststore.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>

This publication is for educational purposes only and is not intended as an offer or solicitation for the sale of any financial product or service. This publication is not designed or intended to provide financial, tax, legal, accounting, or other professional advice since such advice always requires consideration of individual circumstances. If professional advice is needed, the services of a professional advisor should be sought.

Wilmington Trust is a registered service mark used in connection with various fiduciary and non-fiduciary services offered by certain subsidiaries of M&T Bank Corporation including, but not limited to, Manufacturers & Traders Trust Company (M&T Bank), Wilmington Trust Company (WTC) operating in Delaware only, Wilmington Trust, N.A. (WTNA), Wilmington Trust Investment Advisors, Inc. (WTIA), Wilmington Funds Management Corporation (WFMC), and Wilmington Trust Investment Management, LLC (WTIM). Such services include trustee, custodial, agency, investment management, and other services. International corporate and institutional services are offered through M&T Bank Corporation's international subsidiaries. Loans, credit cards, retail and business deposits, and other business and personal banking services and products are offered by M&T Bank, Member FDIC. Wilmington Trust traces its roots to the founding of Wilmington Trust Company in 1903.