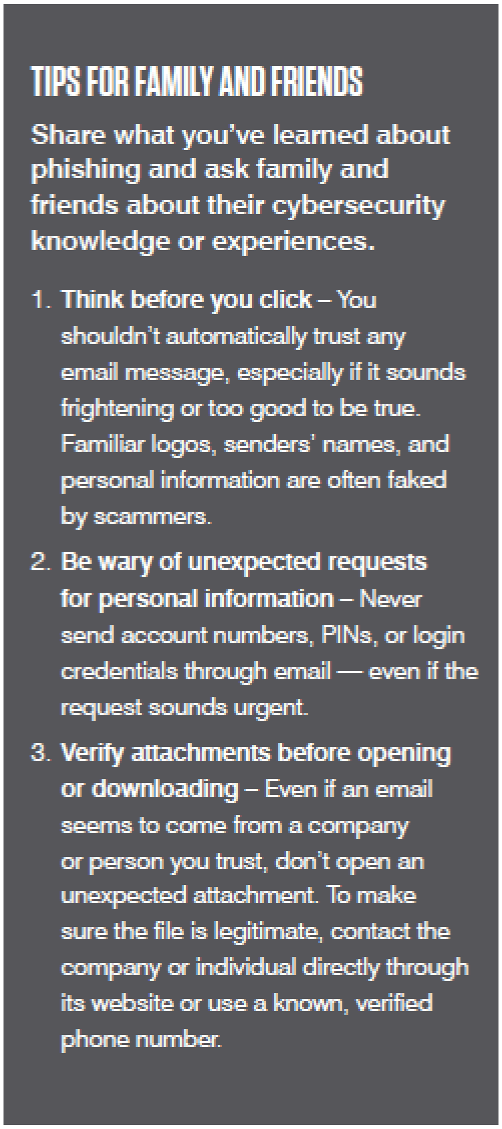
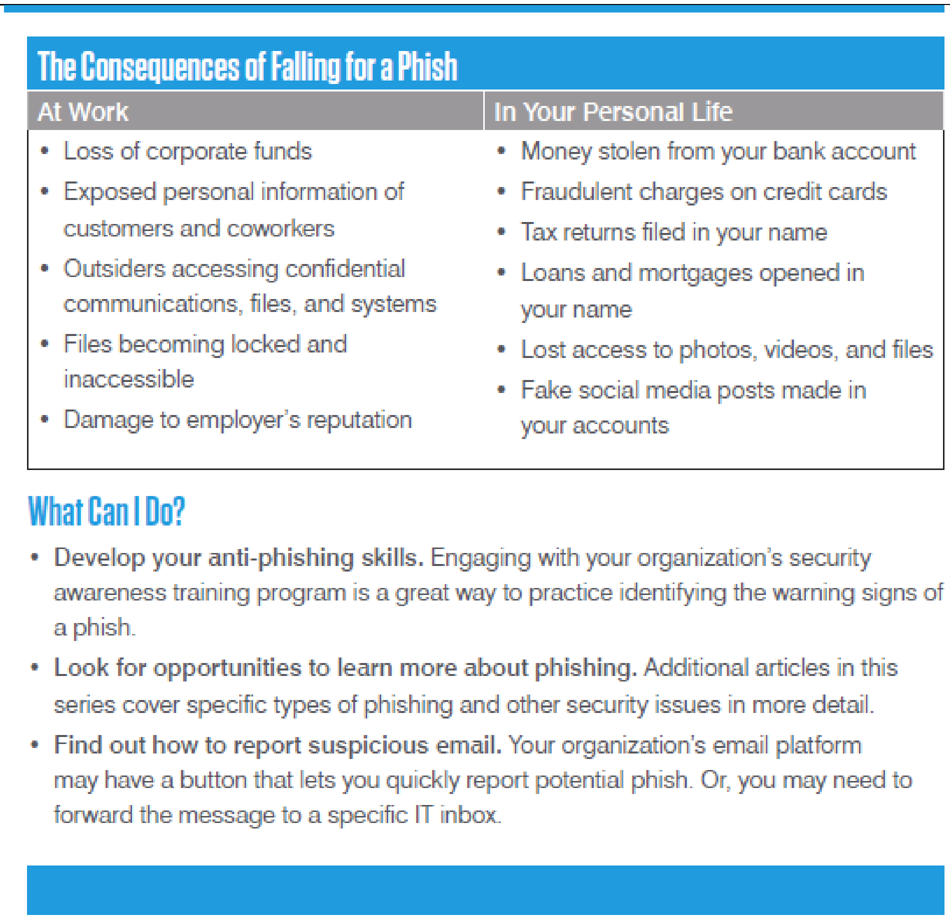
Cybersecurity Tips for family and friends



TIPS FOR FAMILY AND FRIENDS

Share what you've learned about phishing and ask family and friends about their cybersecurity knowledge or experiences.

1. **Think before you click** – You shouldn't automatically trust any email message, especially if it sounds frightening or too good to be true. Familiar logos, senders' names, and personal information are often faked by scammers.
2. **Be wary of unexpected requests for personal information** – Never send account numbers, PINs, or login credentials through email — even if the request sounds urgent.
3. **Verify attachments before opening or downloading** – Even if an email seems to come from a company or person you trust, don't open an unexpected attachment. To make sure the file is legitimate, contact the company or individual directly through its website or use a known, verified phone number.



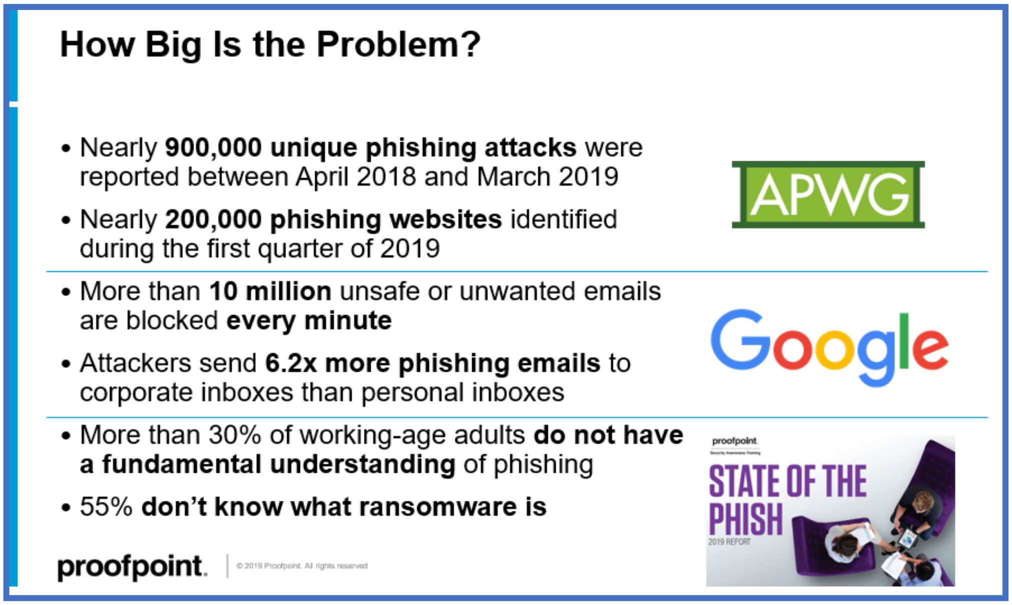
The Consequences of Falling for a Phish

At Work	In Your Personal Life
• Loss of corporate funds • Exposed personal information of customers and coworkers • Outsiders accessing confidential communications, files, and systems • Files becoming locked and inaccessible • Damage to employer's reputation	• Money stolen from your bank account • Fraudulent charges on credit cards • Tax returns filed in your name • Loans and mortgages opened in your name • Lost access to photos, videos, and files • Fake social media posts made in your accounts

What Can I Do?

- **Develop your anti-phishing skills.** Engaging with your organization's security awareness training program is a great way to practice identifying the warning signs of a phish.
- **Look for opportunities to learn more about phishing.** Additional articles in this series cover specific types of phishing and other security issues in more detail.
- **Find out how to report suspicious email.** Your organization's email platform may have a button that lets you quickly report potential phish. Or, you may need to forward the message to a specific IT inbox.

How big is the problem? From the statistics you can see phishing is big business. Still many individuals are not as informed as they need to be in order to stay safe.



How Big Is the Problem?

- Nearly **900,000 unique phishing attacks** were reported between April 2018 and March 2019
- Nearly **200,000 phishing websites** identified during the first quarter of 2019

APWG

- More than **10 million** unsafe or unwanted emails are blocked **every minute**
- Attackers send **6.2x more phishing emails** to corporate inboxes than personal inboxes

Google

- More than 30% of working-age adults **do not have a fundamental understanding** of phishing
- 55% **don't know what ransomware is**

proofpoint

STATE OF THE PHISH

2019 REPORT

proofpoint. | © 2019 Proofpoint. All rights reserved